Diese Website verwendet Cookies von Google, um Dienste anzubieten und den Traffic zu analysieren. Deine IP-Adresse und dein User-Agent werden zusammen mit Messwerten zur Leistung und Sicherheit für Google freigegeben. So können Nutzungsstatistiken generiert, Missbrauchsfälle erkannt und behoben und die Qualität des Dienstes gewährleistet werden.

WEITERE INFORMATIONEN OK

An unending variety of topics

Friday, March 31, 2006

Shared key generation using quasars

This article at The Register is the best layman's description I've seen. The basic idea is that Alice and Bob start by sharing a "key" that is a location and time interval for measuring radio transmissions from the same quasar. The couple (you didn't know that Alice and Bob are an item now?) can then use the voluminous "truly random" data generated by the quasar to generate secret cryptographic keys. Presumably the visible universe has so many quasars that it's sufficiently improbable that the adversary could guess and sufficiently difficult for the adversary to constantly observe all the quasars in order to observe and identify the transmission being observed by Alice and Bob.

There is an interesting discussion about the idea at Bruce Schneier's blog. However, while this discussion addressed several smaller problems that must be solved before this technique can become practical and widespread, the discussion failed to address one issue that should be glaring.

The biggest problem, which must be addressed with any physics-based "truly random" number scheme, is how do we know that these signals are "truly random"? On what physical theories and assumptions is this claim based? How do we know that scientists won't in the future learn more about how quasars work or discover new scientific laws that demonstrate regularity in the data once deemed random? Of course, as any good cryptographer knows, the fact that such data has passed all the statistical tests that we've so far devised is merely suggestive and hardly proves that the data is truly random, any more than it proves that a pseudorandom data stream is secure. There has to be a more basic argument to prove randomness, such as implausibility of >>c communications with respect to causality that would occur if certain quantum phenomena were not truly random.

This is a problem that needs to be addressed for any "truly random" source, but some physical randomness assumptions and arguments are better than others. This is certainly not something we should take on faith or leave to physicists who by "randomness" merely refer to standard statistical tests rather than cryptographic criteria.

See my articles on "true randomness" and the use of statistical tests in cryptography for more about this problem.

Pages

- Home

About Me

Nick Szabo

"A premier thinker about history, law and economics, and the lessons they have for security." -- Adam Shostack, Emergent Chaos

"Szabo comes out with these essays that leave me in awe." -- Brian Dunbar

"Reading material that is eclectic, challenging and endlessly fascinating." -- Sean McGrath, Propylon

"Like most blogs worth my attention, this blog is updated only infrequently. That is because the authors of blogs worth my attention only post when they have something to say that is true, relevant and not already known by their audience. Most of the human race does not have the skill to know when an idea has these three properties. The skill is particularly rare in the fields of politics and economics, which is why this blog is such a rare and valuable thing." -- Richard Hollerith

View my complete profile

Posted by Nick Szabo at 6:48 PM

Newer Post Home Older Post

Blog Archive

- ► 2018 (1)
- ► 2017 (3)
- ► 2016 (4)
- ► 2015 (3)
- ► 2014 (3)
- ► 2013 (3)
- ► 2012 (8)
- ► 2011 (12)
- ► 2010 (9)
- ► 2009 (29)
- ► 2008 (55)
- ► 2007 (47)
- ▼ 2006 (130)
  - ► December (4)
  - ► November (7)
  - ► October (15)
  - ► September (15)
  - ► August (20)
  - ► July (5)
  - ► June (10)
  - ► May (4)
  - ► April (3)
  - ▼ March (11)
    - Off-the-record conversations for the Internet
    - Shared key generation using quasars
    - Corporate origins of the United States
    - Metabolite prediction
    - Estimating inflation
    - Rawlsians' maximin: preposterous risk aversion
    - The Magna Carta, Pt. I
    - Property in everything: some background to the Mag...
    - BlackBerry settlement

Why are wages flat and inequality growing?

Quantum dot control over light and heat

► February (10)

► January (26)

► 2005 (44)

Simple theme. Powered by Blogger.